



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/461,010

12/15/1999

PIERRE CALVEZ

6313

3226

7590

06/27/2006

EDWARD J KONDRACKI  
MILES & STOCKBRIDGE PC  
1751 PINNACLE DRIVE  
SUITE 500  
MCLEAN, VA 221023833

EXAMINER

PICH, PONNOREAY

ART UNIT

PAPER NUMBER

2135

DATE MAILED: 06/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/461,010	CALVEZ ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Ponnoreay Pich	2135	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 13 March 2006.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 20-56 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 20-56 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 April 2000 and 15 September 2005 is/are: a) ☐ accepted or b) ☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)             | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date _____   | 6) <input type="checkbox"/> Other: _____                                    |

### **DETAILED ACTION**

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/13/2006 has been entered.

Claims 1-19 were previously cancelled. Claims 20-56 are pending.

#### ***Response to Amendment and Arguments***

Applicant's amendments and arguments have been fully noted, but are moot in view of new rejections presented below in response to the amendments.

#### ***Drawings***

The drawings submitted on 4/7/2000 and 9/15/2005 are objected to for being informal due to hand written corrections. The drawings are of sufficient quality to proceed with examination, but applicant may at some point wish to obtain the services of a professional draftsman to provide formal and neater drawings.

#### ***Claim Objections***

Claims 20 and its dependent claims are objected to because of the following informalities: Applicant refers to certain items as both "said item" and "the item". The examiner respectfully suggests consistently using either "said" or "the" when referring to the same item. For example, in claim 20, applicant refers to "said second individual certification request" while in claim 23, applicant refers to "the second individual

Art Unit: 2135

certification request”—claim 23 is dependent on claim 20. Applicant may wish to check the other pending claims also for similar minor informalities. Claim 33 is also objected to because the examiner believes applicant meant to recite “creating a new certificate...”. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 20-51 and 53-56 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

1. Claim 20 recites “the one or more attributes” in line 10, which lacks antecedent basis. All subsequent recitation of “the one or more attributes” in claim 20 and its dependent claims are also rejected for lack of antecedent basis. Claim 29 and its dependent claims have the same problem. Claim 51 also has a similar problem.
2. Claim 20 recites “said first individual certification request”, which lacks antecedent basis. All subsequent recitation of “said first individual certification request” in claim 20 and its dependent claims are also rejected for lack of antecedent basis. The examiner assumes applicant meant “said at least one first individual certification request”.
3. Claim 20 recites “said second individual certification request”, which lacks antecedent basis. All subsequent recitation of “said second individual

certification request” in claim 20 and its dependent claims are also rejected for lack of antecedent basis. The examiner assumes applicant meant “said at least one second individual certification request”.

4. Claims 23-25 and 36-39 recite the clause “as well as to model pairs of keys and associated model certificates for the set in question”. This clause does not seem to form a complete thought even taking into account what has previously recited. Further, it is unclear which is “the set in question”. Clarification by applicant is respectfully requested.
5. Claim 29 recites “said individual certification request” which lacks antecedent basis. The examiner assumes applicant meant “said at least one individual certification request”. Any claims dependent on claim 29 which recite “said individual certification request” are also rejected for the same reasons.
6. Claims 30 and 33 recite “the certificate” which lacks antecedent basis. Note that claims 30 and 33 are dependent on claim 29. The examiner assumes applicant may have meant “the first certificate”. Any other recitation of “the certificate” in claims dependent on claim 29 is also rejected for the same reasons.
7. Claim 47 recites “the system”, which lacks antecedent basis. The examiner assumes applicant meant “the computer system”. Any subsequent recitations of “the system” in claims depending on claim 47 are rejected for the same reasons.
8. Any claims not specifically addressed are rejected by virtue of dependency.

***Claim Rejections - 35 USC § 103***

Art Unit: 2135

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 20-22, 29-35, and 45-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Carroll (US 6,105,131).

**Claim 20:**

Ishii discloses:

1. Searching in storage means for at least one user for which a pair of asymmetric keys and an associated certificate must be created (Fig 6 and col 12, lines 28-38).
2. Creating at least one first individual creation and certification request for a pair of asymmetric keys for said user (Fig 6 and col 11, lines 20-62).
3. Transmitting a key generation request corresponding to said at least one first individual creation and certification request to a key generating center, which issues a pair of asymmetric keys in accordance with said key generation request (Fig 6 and col 11, lines 20-62).
4. Creating a public key for said user (col 11, lines 60-62).
5. Creating at least one second individual certification request for public key created for said user (Fig 6, item 417 and col 11, line 63-col 12, line 5).
6. Transmitting a certification request authority request corresponding to said at least one individual certification request to a certification authority and issuing a

first certificate in accordance with said certification authority request (Fig 6 and col 12, lines 6-16 and lines 41-46).

Ishii does not explicitly disclose each user associated with a status associated with an attribute wherein each attribute is capable of having any one of the following values: pending, in progress, process ended with an error message, process done, sending a creation request and done. Ishii also does not explicitly disclose the creation of the at least one individual creation and certification request is based on one or more attributes.

However, Carroll discloses users associated with a status associated with an attribute wherein each attribute is capable of having any one of the following values: pending, in progress, process ended with an error message, process done, sending a creation request and done (Fig 5 and col 7, lines 9-13). Carroll discloses the creation of at least one individual creation and certification request is based on one or more attributes (Fig 5).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Ishii's invention according to the limitations recited in claim 20. One skilled would have been motivated to do so because it would allow a user to determine when a request for a certificate and keys has been processed and the certificate and keys are available for use. One skilled should appreciate that in most systems one would not want to try to use a certificate and associated keys before they are created as this would result in errors.

Art Unit: 2135

**Claim 21:**

Ishii further discloses creating the pair of keys for a given user when said user lacks the pair of keys and the corresponding at least one first individual creation and certification request (Fig 6).

**Claim 22:**

Ishii and Carroll do not explicitly disclose executing said process periodically. However, the examiner take official notice that certificates with corresponding keys which expires and has to be replaced periodically were well known in the art at the time applicant's invention was made. In such systems, the certification and key creation process would have to be executed periodically.

It would have been obvious to one skilled in the art to further modify Ishii's invention such that the certificates and corresponding keys expired periodically, thus new certificate and keys would have to be generated by executing said process periodically. One skilled would have been motivated to do so because periodic replacement of keys and certificates ensures greater security. It is the same concept of why it is recommended that people change their password periodically.

**Claim 45:**

With respect to claim 45, the limitation "comprising performing the encoding of one or more extensions in accordance with one or more given rules and of entering the encoded extension or extensions into the individual certification request during the creation of said individual certification request" is met by Ishii on column 11, lines 63-67 and column 12, lines 1-3.



**Claim 46:**

With respect to claim 46, the limitation “changing the value of the attribute contained in each of the individual first and second requests to indicate status of the process” is met by Ishii on Fig. 20 and 21.

**Claim 53:**

As per claim, the limitation of creating a pair of keys for a given user when a certificate issued in response to a certification authority request for a pair of keys for said user intended for an identical use has been revoked and a new pair of keys has been requested is not explicitly disclosed by Ishii. However, the examiner take official notice that certificate and keys which have an expiry date and are revoked were well known in the art at the time applicant's invention was made. It was further well known to issue another set of keys and certificate when the old ones expired and new ones were needed for an identical purpose.

At the time applicant's invention was made it would have been obvious to further modify Ishii's invention according to the limitations recited in claim 53 because periodically revoking old certificates and keys and issuing new ones for identical purposes would ensure greater security.

**Claim 55:**

Carroll further discloses periodically activating a local registration authority to perform the search step (col 8, lines 29-31).

**Claim 56:**

Ishii and Carroll do not explicitly disclose the activation period is modifiable. However, the examiner take official notice that modifying the time period that various automated processes are done are well known in the art. For instance, the timer for a computer's screen saver is a modifiable option.

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Ishii's invention such that the activation period is modifiable. One skilled would have been motivated to do so because it would allow an administrator to control the amount of system resource used for the automated search so that other processes in the system are not starved of the resources.

**Claim 29:**

As per claim 29, it is broader than claim 20. However, the limitations recited in claim 29 are substantially similar to what is found in claim 20 and claim 29 is rejected for the same reasons given in claim 20.

**Claim 30:**

Ishii further discloses creating the certificate for a given user when said user lacks the pair of keys and the corresponding at least one first individual creation and certification request (Fig 6).

**Claims 31-32:**

Claims 31-32 recite limitations substantially similar to what is recited in claim 22 and are rejected for the same reasons given in claim 22.

**Claims 33-35:**

Ishii further discloses creating a new certificate for a given user when the first certificate expires (col 12, lines 17-50).

**Claim 54:**

Claim 54 recites limitations substantially similar to what is recited in claim 53 and is rejected for the same reasons.

**Claim 47:**

Ishii discloses:

1. A key generating center for creating at least one pair of keys at the request of a local registration authority with which the key generating center communicates (Fig 5, item 130).
2. At least one certification authority to which the system has access for creating a certificate at the request of the local registration authority (Fig 5, item 140).
3. Means for automating, based on one or more attributes associated with one or more users, the creation and/or certification of at least one pair of keys for each user managed by the computer system (Fig 5, item 141-145).

Ishii does not explicitly disclose each attribute is capable of having any one of the following values: pending, in progress, process ended with an error message, process done, sending a creation request and done. However, this limitation is disclosed by Carroll (Fig 5 and col 7, lines 9-13).

In light of Carroll's teachings, it would have been obvious to one skilled in the art to modify Ishii's invention according to the limitations recited in claim 47. One skilled

Art Unit: 2135

would have been motivated to incorporate Carroll's teachings within Ishii's invention for the same reasons given in claim 20.

**Claim 48:**

Ishii further discloses a central management service for creating, updating and consulting objects and users managed by said computer system; a local registration authority for handling the creation and/or the certification of keys intended for the objects and the users; a central security base containing the users and the objects managed by the computer system with which the local registration authority communicates; a key generating center for creating at least one pair of keys at the request of the local registration authority with which the key generating center communicates; and at least one certification authority to which the computer system has access for creating a certificate at the request of the local registration authority (Fig 5).

**Claims 49-50:**

Claims 49-50 recite a limitation directed towards a wake up mechanism for implementing the method claim 55. Claims 49-50 are rejected for substantially the same reasons given in claim 55.

**Claim 51:**

The limitations recited in claim 51 are similar to what is recited in claim 20 and are rejected for substantially the same reasons. The difference is that claim 51 uses symmetric key cryptography while claim 20 uses asymmetric key cryptography. However, both types of cryptosystems were well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify the

Art Unit: 2135

method recited in claim 20 so that it uses symmetric key cryptography instead of asymmetric key cryptography. One skilled would have been motivated to do so because symmetric key systems are faster than asymmetric key systems and sometimes speed is preferred to greater security.

Note that claim 51 also has the additional limitation of issuing by said key generating center a symmetric key in accordance with said transmitted key generating request. However, Ishii also discloses issuing by the key generating center a key in accordance with said transmitted key generating request (Fig 6, item 435).

**Claim 52:**

The limitations recited in claim 52 are similar to what is recited in claim 47 and are rejected for substantially the same reasons. The difference is that claim 52 uses symmetric key cryptography while claim 47 uses asymmetric key cryptography. However, both types of cryptosystems were well known in the art at the time applicant's invention was made. It would have been obvious to one skilled in the art to modify the system of claim 47 so that it uses symmetric key cryptography instead of asymmetric key cryptography. One skilled would have been motivated to do so because symmetric key systems are faster than asymmetric key systems and sometimes speed is preferred to greater security.

Claims 23-28 and 36-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Carroll (US 6,105,131) in further view of Van Oorschot (US 6,370,249).

**Claims 23-25:**

Ishii and Carroll do not explicitly disclose the further limitations recited in claims 23-25. However, these limitations are met by Van Oorschot and Aziz

The limitation “wherein the individual first individual creation and certification request and the at least one second individual certification request are created from corresponding multiple creation and certification requests stored in the storage means...” is met by Van Oorschot on column 3, lines 20-38.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Van Oorschot within the combination of Ishii and Carroll. One skilled would have been motivated to do so because it would allow the certification process to be more efficient since requests can be received and queued rather than waiting for one process to fully complete before receiving the next request.

The limitation of the storage is relative to a set of users belonging to a preset list or to a set of users defined by predetermined criteria, as well as to model pairs of keys and associated model certificates for the set in question is also not disclosed by Van Oorschot.

However, note that Ishii discloses that before certification is done, his invention verifies the user’s data to make sure the personal data matches (col 12, lines 28-37).

Art Unit: 2135

This implies that Ishii's invention holds a predetermined list of users and associated predetermined criteria that are used to validate the entered user information.

At the time applicant's invention was made, it would have been obvious to store the requests relative to a set of users belonging to a preset list or to a set of users defined by predetermined criteria, as well as to model pairs of keys and associated model certificates for the set in question in light of Ichii's teachings. One skilled would have been motivated to do so because it would ensure that only authorized users are able to use the certification devices, i.e. in the case where certification is a paid for process.

**Claims 26-28:**

Van Oorschot further discloses searching in each of the multiple creation and certification requests for all of the subjects in a condition such that a pair of keys must be created (col 4, lines 37-47).

**Claims 36-39:**

Claims 36-29 recite limitations that are similar to what is recited in claim 23 and is rejected for substantially the same reasons.

**Claims 40-43:**

Claims 40-43 recite limitations substantially similar to what is recited in claim 26 and are rejected for the same reasons.

Claims 44 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ishii (US 5,768,389) in view of Carroll (US 6,105,131) in further view of Schneier ("Applied Cryptography").

**Claim 44:**

Ishii and Carroll do not explicitly disclose the further limitation recited in claim 44. However, the further limitation is met by Schneier.

The limitation "wherein each multiple request comprises an attribute relative to at least one execution date and in that said process comprising of including in the search only the multiple requests whose expiration date has arrived" is met by Schneier on page 183-184, section 8.10.

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Schneier within the combination of Ishii and Carroll so as to prevent the existence of keys for an extended period of time and hence lessen the likelihood of the keys being compromised as disclosed by Schneier within the above citation.

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Curry et al (US 6,128,740) discloses revocation of certificates and revocation lists.



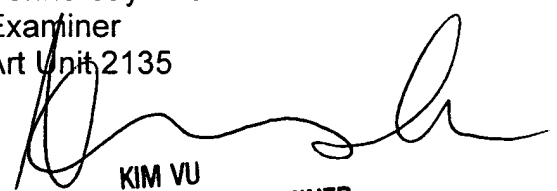
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PP

Ponnoreay Pich  
Examiner  
Art Unit 2135



KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100